УДК 336.717.6

УМАРОВ Андрей Умарович – аспирант 3-го курса, направление «Экономика и управление народным хозяйством», кафедра «Менеджмент» (men_756@mail.ru)

ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ ДАННЫХ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ПРОБЛЕМЫ ИХ СОХРАННОСТИ

Аннотация. Представлен материал о том, для чего нужно организовывать безопасность, сохранность и защиту распространения данных корпоративной информационной системы (ERP).

Ключевые слова: Корпоративная информационная система, безопасность, информация, информационная система.

Umarov A.U., PhD student, 3rd year, Economics and national economy management, «Management» Department Tver (men_756@mail.ru)

ORGANIZATION DATA SECURITY CORPORATE INFORMATION SYSTEMS AND THE PROBLEM OF THEIR PRESERVATION

Abstract. This article presents material about why you need to organize the security, integrity and protection data dissemination of corporate information system (ERP).

Keywords: Corporate information system security, information, information system.

Двадцать первый век стал веком обширного развития в России информационных технологий, которые успешно применяются во многих областях. Польза информационных технологий стала известна уже в самом начале их применения. Автоматизация управления сбытом, информация о проданном и оставшемся на складе товаре, анализ данных, прогноз производства и управление им стали возможными в режиме реального времени.

Польза информационных систем на предприятии стала очевидной. Теперь, когда информатизация стала охватывать предприятия совершенно разных отраслей, суть конкурентоспособности в рыночных отношениях изменилась. Корпоративные информационные системы дали возможность организациям знать то, что происходит с их производством в режиме реального времени, а это в свою очередь дает возможность сразу определить, какие части организации являются слабыми, а какие –сильными. Также появляется возможность вводить новые управленческие решения для улучшения производства, роста продаж, т. е. для увеличения прибыли. Все это открывает новые возможности не просто удержаться на рынке, но и, более того, добиться высокой конкурентоспособности.

После того как организация адаптировала производство на имеющем-ся рынке, автоматизация процессов тоже приобретает большое значение. Быстрота и точность происходящих процессов определяют конкурентоспособность предприятия. После того как предприятие организовано, производство и продажа товаров и услуг автоматизированы, организация может функционировать достаточно успешно в своей области, но возникает другая проблема, из-за которой на данном рынке могут появится конкуренты-клоны (организации с подобной структурой управления, подобным производством и любыми другими подобными характерными признаками). Несложно представить, из-за чего такое может произойти.

Строго отлаженная структура организации, специально обученный персонал, автоматизированность поставок и другие ключевые моменты естественно являются залогом успешной деятельности, но одним из главнейших моментов является также сохранность коммерческой тайны.

Суть работы многих организаций зависит от сохранности коммерческой тайны. Как правило, в сетях крупной организации в обязательном порядке присутствует информация, содержащая тайну. В зависимости от характера деятельности компании это может быть коммерческая, врачебная, банковская тайна, персональные данные; иногда корпорации работают с данными, содержащими государственную тайну.

Кроме того, всегда нужно учитывать вариант, что корпоративная система в будущем может быть причислена к категории ключевых систем информационной инфраструктуры страны. Поэтому сохранение и неразглашение корпоративной информации приобретает глобальный характер, и от сохранности коммерческой тайны может зависеть дальней-шее

функционирование организации. Корпоративная сеть нуждается в защите не только от кражи информации, но и от искажения и порчи программ, документов, баз данных и другой важной для организации информации.

Для систем управления корпоративным контентом следует также предусмотреть отдельный периметр безопасности и специализированную систему защиты.

Периметр создается с помощью классических решений и методо-логии по информационной безопасности – путем внедрения средств меж-сетевого экранирования, создания защищенных подключений по техно-логиям VPN, Remote Access VPN и SSL VPN и усиления процедур аутен-тификации (например, многофакторная аутентификация). В зависимости от требований, связанных с непрерывностью функционирования, в состав решения могут быть включены специализированные системы защиты от DDoS-атак, такие как Arbor Pravail APS.[1]

При создании специализированной системы защиты следует уделить внимание не только разграничению прав доступа к приложению, базам данных и физической инфраструктуре системы, но и созданию дополнительного контура безопасности.

Для того чтобы своевременно обнаружить и ликвидировать такую угрозу, необходимо проводить аудит вновь созданного исходного кода силами сторонней организации или заказчика.

С каждым годом киберпреступность растет, что отражается на безопасности предприятий, хотя в настоящее время понимание киберугроз усилилось и правоохранительные органы начали принимать соответствующие меры.

Совместная работа в этом направлении становится необходи-мостью, чтобы избежать потерь от кибератак. Мировое сообщество страдает из-за отсутствия общей поддержки. Вероятность распада бизнеса увеличивается из-за высокой цены на меры предотвращения бесчисленных кибератак.

Библиографический список

1. Колыбельников, А. http://bit.samag.ru/archive/article (по состоянию на 14.02. 2015 г.).

2. Европейский журнал оперативное исследование 146 (2003) www.elsevier.com/locate/dsw (по состоянию на 14.02.2015 г.)

3. Лондон, Дж. Управление информационными системами. / Дж. Лондон, К. Лондон, под ред. Д.Р. Трутнева; 7-е изд., сер. «Классика MBA»; пер. с англ. СПб.: Питер, 2005. 912 с.